Spamhaus Block List

Apakah Anda pernah mendengar Spamhaus Block List (SBL)? Atau bahkan pernah berurusan dengan SBL? SBL ini penting untuk diketahui oleh siapa saja yang memiliki website. Sebab SBL bisa memberikan dampak buruk website dan bahkan layanan hosting yang Anda gunakan.

Pada artikel ini saya akan membahas seluk beluk mengenai SBL, dari pengertian SBL, penyebab, akibat, cara mengatasi, hingga cara pencegahannya..

Apa itu SBL (Spamhaus Block List)?

Spamhaus Block List (SBL) adalah database yang berisi alamat IP yang terindikasi melakukan tindakan spam. Seluruh alamat (email dan IP) yang ada di daftar tersebut akan diblokir dari akses ke email.
SBL tidak hanya berisi daftar alamat IP atau domain yang terindikasi spam saja melainkan juga menjalankan sebuah program (*query*) secara terus menerus (*realtime*) untuk mengawasi pertukaran data email di internet.
SBL seperti polisi yang melakukan razia, mengidentifikasi, menandai, dan memblokir terhadap berbagai email yang merusak, mengganggu, dan menyalahi aturan (*term of service*). Sistem ini berjalan 24/7 untuk memastikan pertukaran data email di internet aman.

Penyebab Domain atau Alamat IP Masuk ke Dalam SBL

Ada beberapa macam penyebab domain atau alamat IP masuk ke dalam SBL.

1. Malware

Malware bisa jadi penyebab domain Anda masuk ke dalam daftar blokir SBL. Kebanyakan pengguna tidak sadar. Hal dikarenakan malware bekerja secara otomatis tanpa sepengetahuan pengguna.

Ada berbagai macam malware. Dampaknya pun juga bermacam-macam terhadap sistem yang dimasukinya. Di antara berbagai macam malware, ada malware yang mengakibatkan alamat domain terus mengirimkan email. Tentu saja ini mengakibatkan aktivitas yang tidak biasa.

Kebanyakan email yang berasal dari malware sering gagal dan mengakibatkan catatan pengiriman yang ‘buruk’. Inilah yang mengakibatkan SBL Spamhaus curiga. Jika semakin lama volume kegagalan pengiriman email terus meningkat, SBL akan menambahkan domain Anda ke dalam daftar mereka dan domain dianggap sebagai sumber email spam.

2. Mass Email

Mass email atau terkadang dikenal sebagai bulk email merupakan email yang dikirimkan dalam grup yang cukup besar dalam satu waktu. Biasanya email ini mengandung pesan promosi atau iklan yang dikirimkan dalam jumlah yang besar dalams satu waktu.

Pengguna iklan pada umumnya menganggap bahwa pemasaran secara pribadi dan otomatis merupakan cara yang paling efektif. Mass email dianggap bisa menyampaikan pesan yang tepat kepada orang yang tepat pada waktu yang tepat.

Sayangnya mass email dapat berdampak negatif kepada penggunanya jika tidak hati-hati. Mass email justru menjadi email spamming ketika email yang dikirimkan tidak relevan. Selain itu ada beberapa penyebab lain email dianggap sebagai spam, seperti domain tidak terverifikasi (belum terpercaya), isi tidak relevan, banyak email gagal, dan lain sebagainya.

Jadi sebelum melakukan pengiriman email secara massal pastikan bahwa email yang dikirimkan ukurannya tidak terlalu besar dan penerima merupakan user yang aktif sehingga email yang dikirimkan tidak terjadi *bouncehback* (mental).

3. Melakukan Praktek Spamming

Penyebab terakhir domain Anda masuk ke dalam daftar SBL tentu saja karena dengan sengaja mengirimkan email spam. Email promosi atau iklan dalam jumlah yang besar tergolong spam, tapi pada kasus ini yang dimaksud dengan email spam adalah email yang dikirimkan dengan maksud merusak atau bahkan mencoba untuk membobol keamanan pengguna lain.

Email spam biasanya jumlahnya cukup besar, berisi link, atau melalui alamat domain yang tidak biasa. Pengiriman email dengan ukuran file yang cukup besar biasanya bertujuan untuk memenuhi folder penyimpanan lawan. Sedangkan link yang berada di

dalam email terkadang dijadikan sebagai pintu masuk penyerang untuk mengambil hak akses ke dalam email.

Tentu saja email dengan link dan ukuran yang cukup besar sangat mudah terdeteksi sebagai spam. SBL akan mencurigai domain alamat email berasal dan memasukkannya ke dalam daftar SBL jika terbukti sebagai email spam.

Bahaya SBL

Secara garis besar, ada beberapa bahaya SBL yang perlu Anda ketahui.

1. Terblokirnya akses keluar masuk email

Umumnya SBL akan memblokir koneksi yang berhubungan dengan email Anda. Jadi seluruh aktifitas email tidak dapat berjalan dengan baik. Tentu saja hal ini akan berpengaruh terhadap kelancaran proses bisnis.

Pada tahap awal SBL hanya akan memblokir domain Anda. Namun jika tidak ada penanganan segera, SBL akan memblokir seluruh akun yang ada di range IP sama dengan domain Anda. Sehingga dapat merugikan bagi layanan hosting dan seluruh klien yang berada di IP range tersebut. Oleh karena itu, Niagahoster akan mengambil tindakan segera dengan melakukan suspend permanen terhadap website yang terkena Spamhause Block List.

2. Menurunkan tingkat keabsahan domain

Selain itu dampak akibat terdeteksi SBL adalah terblokirnya segala aktivitas pengiriman email dari domain maupun alamat IPs yang masuk di dalam Spamhaus data. Tidak hanya menolak segala email yang dikirimkan, domain maupun alamat IPs tersebut bisa menjadi alamat yang tidak dipercaya oleh jaringan internet.

Hal ini mengakibatkan segala aktivitas yang berhubungan dengannya akan terganggu, seperti prioritas pengiriman dan sejenisnya. Meskipun belum terbukti secara valid, domain atau IPs yang masuk ke dalam SBL juga bisa menurunkan peringkat di dalam mesin pencari.

3. Secara tidak langsung menurunkan pendapatan

Bagi Anda yang menggunakan email sebagai alat komunikasi utama, tentu saja permasalahan SBL dapat mengakibatkan kerugian yang cukup besar karena email

yang berasal dari klien atau rekan kerja tidak dapat Anda terima. Bahkan, Anda pun tidak dapat menerima email dari sumber yang terpercaya sekali pun.

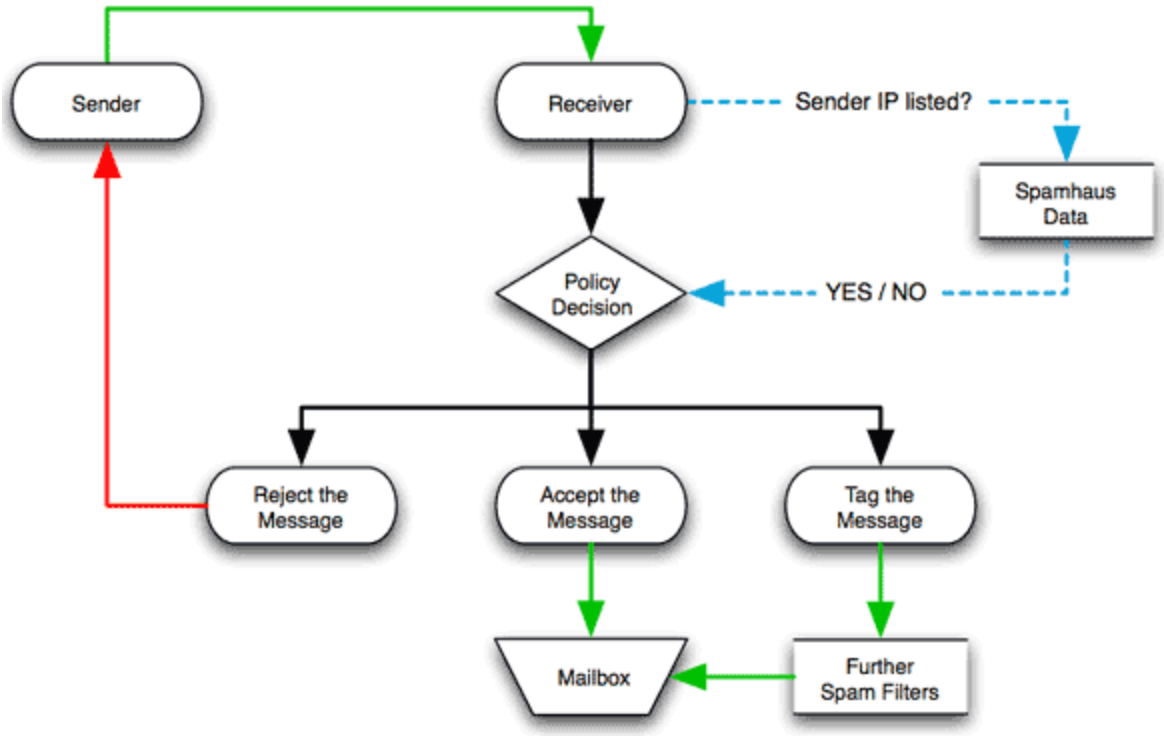
Bagaimana pun, seperti sistem penyaring email lainnya, SBL mempunyai potensi untuk memblokir atau menolak email yang berasal dari alamat yang terpercaya. Contohnya ketika mereka mengirimkan email dari IP di bawah kontrol spammer atau menggunakan IPs yang terindikasi menggunakan Spam Service. Tingkat kesempatan email terpercaya untuk bisa lolos dari kasus tersebut sangat kecil.

Pada kasus seperti itu, biasanya Spamhaus akan menghubungi penyedia layanan ISP dan memberikan informasi terkait aktivitas spam. Tindakan ini untuk menghapus alamat IP atau domain mereka dari daftar blokir. Tentu saja ini dilakukan untuk mengantisipasi terblokirnya pengguna yang sebenarnya tidak bermasalah.

Namun jika penyedia layanan ISP terbukti mendukung kegiatan spammer, Spamhaus akan menandai penyedia tersebut sebagai layanan ‘Spam Support Service’. Bahkan akan mendaftar seluruh layanan yang berada di bawahnya ke dalam daftar blokir.

Cara Kerja SBL

Bagaimana sih SBL bekerja 24/7 hari untuk mengawasi lalu lintas di internet? Supaya lebih jelas, Anda dapat melihat bagan di bawah ini untuk memahami bagaimana cara kerja SBL ketika menangani email.



Jadi, SBL (Spamhaus data) berfungsi sebagai validator atau sistem yang melakukan pengecekan email yang sedang dalam proses pengiriman. Penerima meminta Spamhaus untuk melakukan pengecekan apakah domain atau IP dalam sumber email terdapat di dalam Spamhaus Data. Kemudian Spamhaus memberikan informasi secara otomatis.

Spamhaus tidak mempunyai kontrol penuh bagaimana penerima memperlakukan email yang sudah terdaftar di dalam SBL.

Penerima email mempunyai wewenang secara penuh untuk menentukan apakah email tersebut wajib masuk ke dalam inbox, spam, atau ditolak. Jika email yang sudah terlalu banyak di-tag sebagai email spam, lama kelamaan sistem akan menandai sumber email (domain atau alamat IPs) sebagai pengirim spam dan menolak segala email yang diterima dari domain atau IPs tersebut.

Cara Mendeteksi SBL

Pada kasus tertentu, technical support di Niagahoster terkadang menerima komplain dari klien karena sama sekali tidak bisa mengirimkan email. Tidak hanya satu klien,

tetapi belasan klien di dalam satu IP yang sama. Tentu saja hal ini menimbulkan pertanyaan.
Setelah melakukan pengecekan, ternyata ada domain yang masuk ke dalam list SBL sehingga membuat akun lain dengan alamat IP yang sama terblokir.

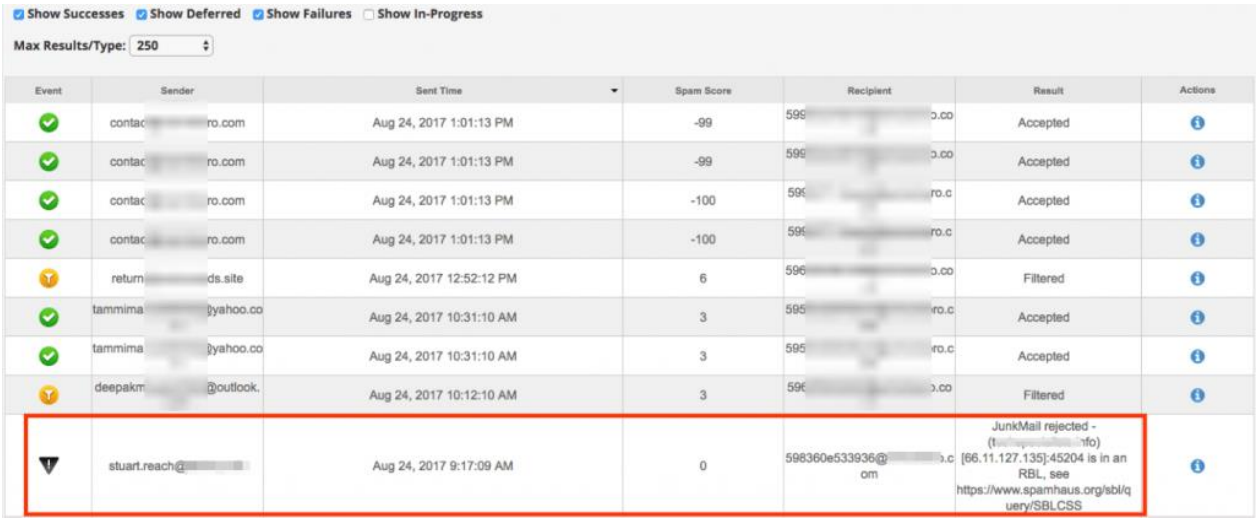
Inilah mengapa kasus yang berhubungan dengan SBL cukup berbahaya karena bisa merugikan pengguna dan juga penyedia layanan hosting yang salah satu penggunanya masuk di dalam daftar SBL.

Anda tidak perlu menghubungi penyedia layanan hosting Anda untuk melakukan pengecekan SBL, karena Anda bisa mengeceknya sendiri terlebih dahulu.

Cara mendeteksi SBL paling mudah adalah dengan membuka fitur Track Delivery di cPanel. Selain itu, Anda juga bisa langsung melakukan pengecekan domain atau alamat IPs melalui Blocklist Removal Center yang tersedia di website Spamhaus.

1. Pengecekan menggunakan cPanel

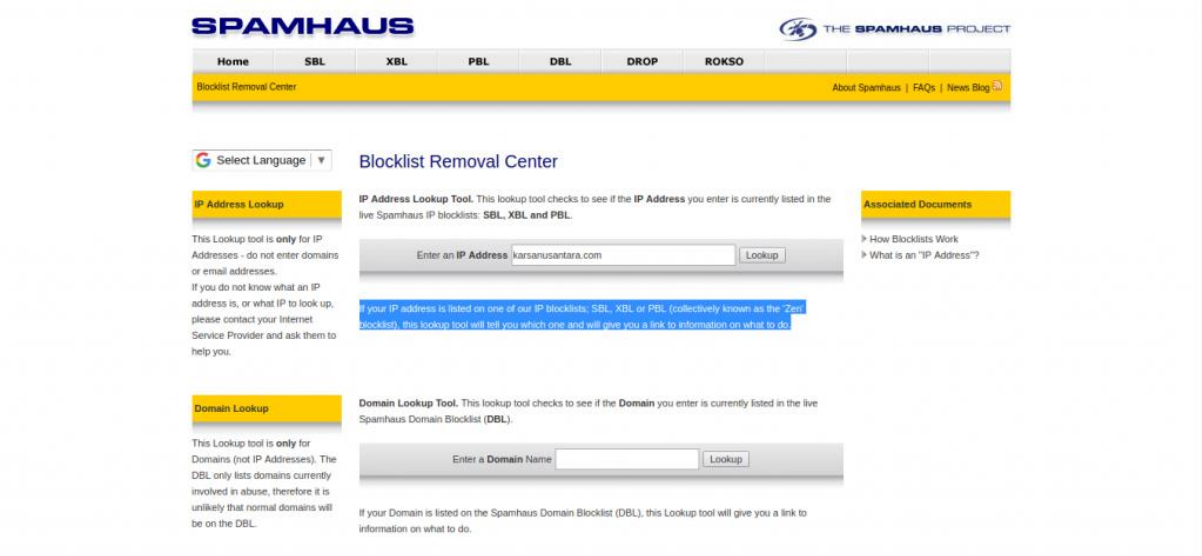
Jika Anda mempunyai akses ke cPanel, proses pengecekan SBL proses pengecekan Spamhaus cukup mudah. Silakan akses cPanel Anda kemudian buka fitur **Track Delivery**.
Pada fitur ini terdapat informasi pengiriman dan penerimaan email. Anda dapat melihat tanggal pengiriman email, email pengirim, dan email tujuan. Selain itu, Anda juga dapat melihat apakah email yang Anda terima atau kirimkan bermasalah atau tidak.



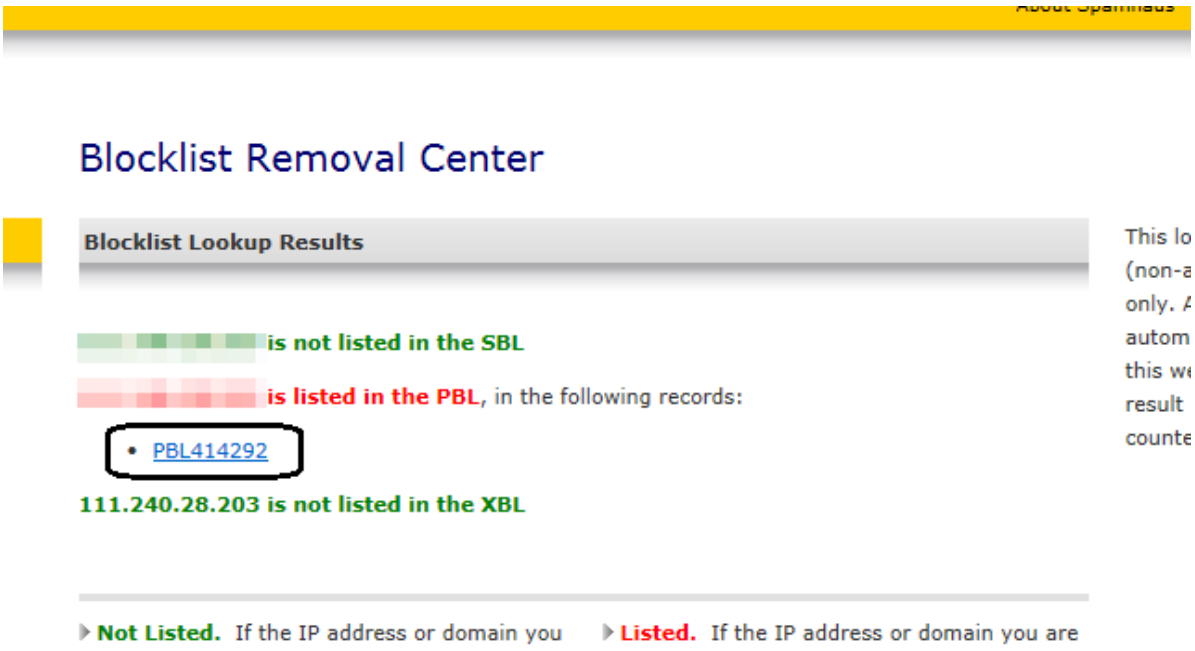
Email yang bermasalah biasanya akan ditandai dengan **tanda seru** (⚠). Tidak hanya itu, pada keterangan laporan akan menginformasikan alasan email tersebut bermasalah. Email yang bermasalah dengan SBL akan menyertakan link yang mengarah ke Spamhaus dengan keterangan seperti **JunkMail rejected**.

2. Pengecekan melalui situs Spamhaus

Sedangkan untuk pengecekan SBL melalui website Spamhaus, silakan akses fitur Blacklist Removal Center. Di dalam fitur ini terdapat IP Address Lookup Tool dan Domain Lookup Tool. Keduanya dapat Anda gunakan untuk mengecek indikasi SBL.



Jika Anda ingin mengecek SBL pada alamat IP, gunakan IP Address Lookup Tool. Sedangkan Domain Lookup Tool berguna untuk untuk mengecek SBL di domain. Keduanya akan mengecek apakah alamat IP maupun yang akan masukkan pada saat ini terdaftar di dalam list blokir Spamhaus: SBL, XBL, dan PBL (biasa dikenal sebagai Zen blocklist).



Jika domain atau alamat IP Anda terdaftar di dalam daftar blokir di Spamhaus atau Zen Blocklist, tools lookup ini akan memberi Anda informasi alasan terblokir dan memberikan Anda link ke informasi langkah apa saja yang perlu Anda lakukanGambar di atas merupakan contoh hasil pengecekan domain dan alamat IP yang ternyata masuk ke dalam daftar list SBL diblokir.

Terdapat dua status pengecekan yang akan Anda lihat, yaitu ***Not Listed*** dan ***Listed***.

- **Status Not Listed**. Jika alamat IP atau domain yang Anda memunculkan pesan **'Not Listed'** pada hasil pengecekan di atas, domain maupun alamat IP tidak termasuk di dalam daftar blokir Spamhaus.
- **Status Listed**. Jika domain atau alamat IP pada proses pengecekan menghasilkan keluaran **'Listed'**, berarti masuk ke dalam daftar blokir. Spamhaus juga akan memberikan informasi detail alasan mengapa domain atau alamat IP Anda masuk dalam daftar blokir ini beserta panduan untuk menanganinya.

Cara Membersihkan SBL (*Delisting*)

Meskipun membutuhkan waktu yang cukup lama, Anda bisa menghapus domain atau IPs dari SBL.

1. Atasi penyebab domain atau IPs masuk ke dalam SBL.

Jika Anda masuk ke dalam SBL, ini berarti Anda masuk ke dalam mode yang cukup ‘menakutkan’. Kenapa? Karena Spamhaus akan mengganti proses pengiriman dan menghapuskan Anda dari prioritas pengiriman.

Jadi langkah pertama yang perlu Anda lakukan adalah menghentikan terlebih dahulu aktivitas pengiriman email. Anda bisa menggunakan Spamhaus Lookup untuk mencari tahu informasi alasan email Anda tergolong ke dalam spam dan domain atau alamat IPs yang terkena dampaknya.
Kemudian, cari tahu informasi apa yang sebelumnya Anda kirimkan dalam jumlah yang besar. Hal ini biasanya sebuah iklan promosi, informasi penting, atau sejenisnya yang dikirimkan dalam jumlah yang banyak kepada pelanggan atau pengguna layanan Anda. Lakukan pengecekan dan memastikan bahwa semua sudah dalam kondisi baik/tidak bermasalah.

2. Komunikasikan masalah ini dengan berbagai divisi yang berhubungan dengan klien.

Komunikasi ini sangat penting karena seluruh tim harus memperhatikan ini sebagai situasi yang cukup mendesak. Maka dari itu, Anda perlu memastikan bahwa orang yang mengelola email paham betul apa yang terjadi.

Anda juga bisa mengomunikasikan permasalahan ini kepada pengelola domain dan website atau penyedia layanan email. Bagi penyedia layanan email tentu saja ini akan menjadi sesuatu yang penting karena bisa mempengaruhi pengguna lain di dalam satu IPs yang sama.

3. Memperbaiki dan mengelola permasalahan yang muncul.

Jika Anda bingung harus memulai dari mana, Anda bisa menggunakan panduan langkah demi langkah di bawah ini untuk melakukan audit atau pengecekan di dalam sistem atau infrastruktur.

- **Periksa Sistem Infrastruktur**
  Pastikan bahwa Anda mendapatkan feedback atau bounce berisi informasi penolakan yang berasal dari email penerima. Feedback tersebut perlu karena untuk memastikan permasalahan yang Anda hadapi. Namun Anda perlu menghapus feedback secara berkala supaya tidak menjadi sampah di dalam sistem email Anda.

- **Periksa List Acquisition**
  Periksa dan pastikan bahwa segala layanan atau proses yang berjalan di dalam sistem acquisition sudah berhenti (stop). Anda juga perlu memastikan bahwa email penerima benar-benar masih aktif dan dapat menerima email.

- **Hapus Subscribers yang Sudah Inactive**
  Anda perlu membuat peraturan untuk mensuspend pengguna yang sudah tidak aktif lama, jika belum mempunyainya. Hal ini cukup penting untuk menyaring email-email subscriber yang sudah tidak aktif.

  Anda juga bisa menerapkan proses re-engagement untuk menarik perhatian pengguna subscriber yang sudah lama tidak aktif. Jika tidak ada balasan dari mereka, Anda bisa langsung menghapusnya dari daftar penerima email.

- **Monitor Secara Berkala**
  Terakhir yang tak kalah penting yaitu pengecekan secara berkala. Anda tidak perlu menunggu agar Spamhaus mencatat domain atau IPs yang Anda gunakan. Maka dari itu, cara yang paling mudah untuk mengatasi supaya Anda tidak masuk ke dalam lingkaran SBL adalah dengan mencegahnya.

  Pastikan Anda untuk memantau berbagai macam komplain, pengguna dengan rating yang jelek, dan jebakan spam. Jika Anda bisa mengelola berbagai macam penyebab ini dengan baik, Spamhaus akan memastikan bahwa domain atau IPs Anda terkelola dengan baik.

4. Gunakan beberapa *checklist* ini pada waktu melakukan proses delist.

- Konfirmasikan IPs/domain yang terdaftar di dalam SBL
- Identifikasi IPs/domain yang terdampak dan mengalami gagal pada waktu proses pengiriman email.
- Komunikasikan permasalahan ini dengan Admin sistem Anda dan layanan penyedia server email.
- Review email terbaru yang dikirimkan dan lihat kemungkinan sebab yang memicu domain terdaftar di dalam SBL.
- Perbaiki masalah yang membuat domain didaftar di SBL.
  Setelah Anda sudah menjalankan beberapa persyaratan di atas. Untuk proses delist dari Spamhaus, buka halaman lookup Spamhaus kemudian ikuti instruksi untuk melakukan proses delist. Ketika Anda mengisi sebuah form di dalamnya, pastikan

Anda mengkonfirmasi bahwa Anda sudah menyelesaikan permasalahan yang menyebabkan domain atau IPs Anda terblokir oleh SBL.

Namun perlu diketahui bahwa Spamhaus mempunyai wewenang apakah pengajuan delist Anda dapat diterima atau tidak. Jadi proses ini tidak mesti dapat langsung menyelesaikan permasalahan Anda dengan Spamhaus.

Cara Mencegah Masuk ke SBL

Nah! Ketika domain Anda tidak masuk ke dalam daftar SBL atau sudah dihapuskan dari daftar tersebut, tentu saja perlu dilakukan langkah pencegahan. Langkah ini belum tentu mengamankan 100% dari SBL, tapi cukup layak Anda terapkan.

1. Bersihkan website Anda dari malware

Anda perlu memastikan bahwa website bersih dari berbagai macam malware. Selain itu, pastikan juga program atau aplikasi yang Anda tambahkan di dalam website aman atau tidak disusupi dengan script yang berbahaya. Contohnya adalah plugin, tema, script widget, dan lain sebagainya.

Baca juga: **10+ Plugin Security WordPress Terbaik dan Gratis**

Untuk mengecek apakah ada malware di website atau tidak, Anda dapat menggunakan panduan cara menghilangkan malware website di blog kami.

2. Pastikan email berkualitas

Pada saat mengirimkan email, pastikan bahwa email yang Anda kirimkan berkualitas. Ini berarti email menggunakan tata bahasa, konten, dan susunan yang baik. Hal ini untuk mencegah banyaknya Gunakan beberapa checklist ini pada waktu melakukan proses delist.email yang gagal dikirimkan atau dicurigai oleh SBL sebagai email yang berbahaya.

Penutup

Domain atau IPs yang masuk ke dalam SBL bisa dikategorikan permasalahan yang cukup serius. Anda tidak dapat mengirimkan email selama alamat IP atau domain masih terdaftar di dalam SBL. Tidak hanya itu, prioritas maupun tingkat validitas domain Anda menurun karena segala yang masuk ke dalam SBL diidentifikasi sebagai penyebar spam atau spammer (aku pengirim spam).

Selain itu, Anda perlu menjadikan informasi SBL ini sebagai permasalahan bersama karena tidak hanya melibatkan satu divisi saja melainkan bisa mencakup seluruh divisi. Selain itu, SBL tidak hanya merugikan Anda saja melainkan penyedia layanan

hosting, maupun pengguna lainnya. Maka dari itu sangat penting untuk melakukan komunikasi dengan berbagai pihak untuk menentukan langkah yang perlu diambil.

Demikian artikel mengenai SBL, dampak, dan cara mengatasinya. Semoga artikel ini bermanfaat untuk Anda dan mudah Anda pahami. Jika masih ada pertanyaan jangan sungkan untuk meninggalkannya melalui kolom komentar di bawah ini, atau jika Anda menyukai artikel dari kami silakan melakukan *subscribe* untuk mendapatkan informasi terbaru yang akan terbit setiap harinya.

DAFTAR PUSTAKA

Yasin K . 2021. Apa Itu Spamhaus Block List dan Mengapa Berbahaya?. Diakses pada tanggal 25 Januari 2021. Dari laman https://www.niagahoster.co.id/blog/apa-itu-sbl/?amp=1